Claim Listing

Please cancel claims 1-21.

Please add the following new claims:

22. (New) A secure processing system, comprising:

a main processor unit (MPU) coupled to a processor bus;

an attached processor complex (APC) coupled to the processor bus and comprising:

a local store configured to store computer instructions and data;

an attached processor unit (APU) coupled to the local store;

wherein the APC is configured to receive commands from the MPU via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state; and

wherein in response to a LOAD command received from the MPU, the APC is configured to transition from the non-isolated state to the isolated state, to partition the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU, to transfer a set of computer instructions or data into the isolated section of the local store, and to use the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key.

23. (New) The secure processing system as recited in claim 22, wherein secure processing is performed within the isolated section of the local store of the APC.

24. (New) The secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is not accessible by the MPU.

25. (New) The secure processing system as recited in claim 22, wherein the cryptographic master key stored in the APC is unique to the secure processing system.

26. (New) The secure processing system as recited in claim 22, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store.

27. (New) The secure processing system as recited in claim 22, wherein when the APC is operating in the isolated state, the APC is configured to respond to an EXIT command received from the MPU by clearing the isolated section of the local store and eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store.

28. (New) The secure processing system as recited in claim 22, wherein the APC is configured to use the other cryptographic key to authenticate or decrypt another set of computer instructions or data.

29. (New) The secure processing system as recited in claim 22, wherein the APC further comprises a bus interface unit (BIU) coupled to the processor bus, and wherein local store and the APU are coupled to the BIU.

30. (New) The secure processing system as recited in claim 29, wherein the BIU comprises a load/exit state machine (LSEM) configured to store the cryptographic master key.

31. (New) A method for carrying out secure processing, comprising:

providing a main processor unit (MPU), a processor bus, and an attached processor complex (APC), wherein the APC comprises a local store configured to store computer instructions and data and an attached processor unit (APU) coupled to the local store;

configuring the MPU to drive a LOAD command on the processor bus in the event secure processing is required;

coupling the MPU to the processor bus;

configuring the APC to receive the LOAD command via the processor bus, to store a cryptographic master key, and to operate in a non-isolated state and an isolated state;

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state;

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU;

transferring a set of computer instructions or data into the isolated section of the local store;

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic key; and

coupling the APC to the processor bus.

32. (New) The method as recited in claim 31, wherein the secure processing is carried out within the isolated section of the local store of the APC.

33. (New) The method as recited in claim 31, wherein the cryptographic master key stored in the APC is not accessible by the MPU.

34. (New) The method as recited in claim 31, wherein the coupling of the MPU and the APC to the processor bus forms a processing system, and wherein cryptographic master key stored in the APC is unique to the processing system.

35. (New) The method as recited in claim 31, wherein when the APC is operating in the non-isolated state, the general access section occupies the entire local store.

36. (New) The method as recited in claim 31, further comprising:

configuring the APC to respond to a received EXIT command when operating in the isolated state by:

clearing the isolated section of the local store; and

eliminating the isolated section of the local store, thereby causing the general access section to occupy the entire local store.

37. (New) The method as recited in claim 31, wherein the configuring the APC to respond to a received LOAD command comprises:

configuring the APC to respond to a received LOAD command by:

transitioning from the non-isolated state to the isolated state;

partitioning the local store into a general access section accessible by the MPU and an isolated section accessible only by the APU;

transferring a set of computer instructions or data into the isolated section of the local store;

using the master key to extract and decrypt a portion of the computer instructions or data stored in the isolated section of the local store, thereby producing another cryptographic; and

using the other cryptographic key to authenticate or decrypt another set of computer instructions or data.